UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/929,178	08/14/2001	Donald P. Matthews JR.	BRCMP008/BP-1567	8980

22434 7590 03/07/2005

BEYER WEAVER & THOMAS LLP
P.O. BOX 70250
OAKLAND, CA 94612-0250

EXAMINER	
POPHAM, JEFFREY D	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 03/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/929,178	MATTHEWS, DONALD P.	
	Examiner	Art Unit	
	Jeffrey D. Popham	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-25* is/are pending in the application.

4a) Of the above claim(s) *11-25* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *01/18/2002* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *20021028, 20030121*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: *20030828*.

Remarks

Claims 1-25 are pending.

Election/Restrictions

1. Restriction to one of the following inventions is required under 35 U.S.C. 121:

I. Claims 1-10, drawn to a method for processing network security protocol packets.

II. Claims 11-17, drawn to a cryptography accelerator chip architecture.

III. Claims 18-25, drawn to an electronic commerce computer network system.

2. Inventions III and I are related as combination and subcombination. Inventions in this relationship are distinct if it can be shown that (1) the combination as claimed does not require the particulars of the subcombination as claimed for patentability, and (2) that the subcombination has utility by itself or in other combinations (MPEP § 806.05(c)). In the instant case, the combination as claimed does not require the particulars of the subcombination as claimed because the subcombination includes the following limitations not appearing in the combination: passing non-pre-padded network security protocol data from the chip to the source in a single pass.

Invention I has separate utility from invention III such as use in a system that authenticates via MACs.

Invention II is a subcombination of invention III, however, it is not patentably distinct from invention III and is therefore not subject to restriction. It will be examined with Invention III.

Because these inventions are distinct for the reasons given above and the search required for Group I contains the classification 713/170, which is not required for Groups II or III, restriction for examination purposes as indicated is proper.

3. Applicant's election without traverse of invention I (claims 1-10) in a telephone interview with Stephen Burbach on 2/23/2005 is acknowledged.

Drawings

4. Figure 1 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g).

5. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(4) because reference characters "603" and "604" have both been used to designate an expansion card.

Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application.

Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Objections

1. Claims 4, 5, and 7 are objected to under 37 CFR 1.75(a) because of the following informalities:

- Claim 4, line 2 and claim 5, line 2 recite the limitation "the data". There is insufficient antecedent basis for this limitation in the claims. For purposes of prior art rejection, they have been construed as "the non-pre-padded network security protocol data".
- Claim 7, line 1 recites the limitation "said calculation of a pad length". There is insufficient antecedent basis for this limitation in the claim. For purposes of prior art rejection, is has been construed as "a calculation of a pad length".

Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1, 2, and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gressel et al. (U.S. Patent 6,060,321) in view of "The SSL Protocol Version 3.0, hereinafter referred to as SSL3spec.

Regarding Claim 1,

Gressel et al. disclose a method of processing data packets, comprising:

Providing a cryptography processing architecture on a chip (Column 3, lines 14-23);

Passing data for both authentication and cryptography operations from a source to said chip (Column 5, lines 50-52);

Conducting, in hardware, authentication and encryption, operations on the data (Column 5, lines 39-43); and

Passing the crypto-processed data from said chip to said source (Column 5, lines 50-52);

Wherein said data is passed between said chip and said source in a single pass (Column 5, lines 39-52).

Gressel et al. do not disclose that the data is non-pre-padded network security protocol data.

SSL3spec, however, discloses that the data is non-pre-padded network security protocol data (Pages 3-4, Section 1 and Page 10, Section 5.0). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the network security protocol of SSL3spec into the crypto chip of Gressel et al. in order to gain cryptographic security between 2 parties, interoperability between differently coded programs, and extensibility to other protocols and methods (Page 4, Sections 2.1, 2.2, and 2.3).

Regarding Claim 2,

Gressel et al. do not disclose that the network security protocol is SSL (v3).

SSL3spec, however, discloses that the network security protocol is SSL (v3) (Pages 3-4, Section 1 and Page 10, Section 5.0). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the network security protocol of SSL3spec into the crypto chip of Gressel et al. in order to gain cryptographic security between 2 parties, interoperability between differently coded programs, and extensibility to other protocols and methods (Page 4, Sections 2.1, 2.2, and 2.3).

Regarding Claim 9,

Gressel et al. disclose that the encryption operations further include decryption operations (Column 5, lines 39-43).

7. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Gressel et al. and SSL3spec in view of "The TLS Protocol Version 1.0", hereinafter referred to as TLSspec.

Gressel et al. as modified by SSL3spec does not disclose the TLS protocol.

TLSspec, however, discloses that the network security protocol is TLS (Pages 3-4, Section 1). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the network security protocol of TLSspec into the crypto chip of Gressel et al. as modified by SSL3spec in order to gain cryptographic security between 2 parties, interoperability between differently coded programs, and extensibility to other protocols and methods (Pages 4-5, Sections 2.1, 2.2, and 2.3).

8. Claims 4-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gressel et al. in view of SSL3spec, further in view of Kaplan et al. (U.S. Patent 6,704,871).

Regarding Claim 4,

Gressel et al. as modified by SSL3spec does not disclose parallel processing of two data packets.

Kaplan et al., however, disclose the step of simultaneously with conducting the cryptography operations on the non-pre-

padded network security protocol data, pre-loading network security protocol data from a second non-pre-padded network security protocol packet onto the chip (Column 37, lines 47-58). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the crypto chip of Kaplan et al. into the crypto chip of Gressel et al. as modified by SSL3spec in order to obtain fast processing through paralleled and pipelined operations.

Regarding Claim 5,

Gressel et al. as modified by SSL3spec does not disclose parallel processing of two data packets.

Kaplan et al., however, disclose the step of simultaneously with conducting the encryption operations on the non-pre-padded network security protocol data, conducting, in hardware, authentication operations on the network security protocol data from the second non-pre-padded network security protocol packet (Column 37, lines 47-58). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the crypto chip of Kaplan et al. into the crypto chip of Gressel et al. as modified by SSL3spec in order to obtain fast processing through paralleled and pipelined operations.

Regarding Claim 6,

Gressel et al. as modified by SSL3spec does not disclose padding and alignment operations.

Kaplan et al., however, disclose that step of conducting, in hardware, authentication and encryption operations on the non-pre-padded network security protocol data comprises conducting padding and alignment operations on the chip (Column 41, lines 16-51). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the crypto chip of Kaplan et al. into the crypto chip of Gressel et al. as modified by SSL3spec in order to facilitate peak encrypt/decrypt performance.

Regarding Claim 7,

Gressel et al. as modified by SSL3spec does not disclose padding operations or a pad engine.

Kaplan et al., however, disclose the step of calculating a pad length for padding operations being conducted by a pad engine component (Column 41, lines 46-51) of the chip architecture (Column 41, line 63 to Column 42, line 3). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the crypto chip of Kaplan et al. into the crypto chip of Gressel et al. as modified by SSL3spec in order to facilitate peak encrypt/decrypt performance (Column 41, lines 17-19).

9. Claims 8 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gressel et al. in view of SSL3spec, further in view of Weiss (U.S. Patent 5,485,519).

Regarding Claim 8,

Gressel et al. as modified by SSL3spec does not disclose MACs.

Weiss, however, discloses that the step of conducting, in hardware, authentication and encryption operations on the network security protocol data comprises feeding back a MAC value calculated during authentication operations for processing in the encryption operations (Column 6, lines 42-53). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the authentication method of Weiss into the crypto chip of Gressel et al. as modified by SSL3spec in order to provide a way to prove the identity of the sender and the integrity of the data.

Regarding Claim 10,

Gressel et al. as modified by SSL3spec does not disclose that decryption happens before authentication.

Weiss, however, discloses that the step of conducting, in hardware, authentication and decryption operations on the network security protocol data comprises feeding back decrypted data for processing in the authentication operations (Column 6, lines 42-48).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the authentication method of Weiss into the crypto chip of Gressel et al. as modified by SSL3spec in order to provide a way to prove the identity of the sender and the integrity of the data.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffrey D. Popham whose telephone number is (571)-272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571)-272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER